OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM

INFORMATION SECURITY BUSINESS CASE

CASE STUDY #3 - SCOUT

6 March 1997

**Further distribution only as directed by
Office of the Manager,
National Communications System (OMNCS)
Customer Service and Information Assurance Division
Information Assurance Branch (N53)**

DCA100-95-D-0104
Delivery Order No. 10
Information Security Business Case
Case Study #3-SCOUT

ABSTRACT

This case study was prepared as part of a larger effort to develop a business case approach to justify funding for network security programs. The case study participant was selected by the Government sponsor of the project from a list of candidates developed by the SAIC project team. The case study presents an overview of the participant organization to include its technical and operational environments; discusses the motivation for establishing a security program; describes the organization's Network and Information Security Program; overviews the participant's business case process; and presents senior management's view of several network and information security issues.

TABLE OF CONTENTS

<u>**Section**</u> <u>**Page**</u>

1 INTRODUCTION 1
1.1 Purpose of the Project 1
1.2 Approach for SCOUT Case Study 2
1.3 Overview of the Report 2

2 OVERVIEW OF THE SCOUT ORGANIZATION 3
2.1 Description of the Business 3
2.2 Description of Network and Information Systems Environment 4

3 MOTIVATION(S) FOR ESTABLISHING SECURITY PROGRAM 6

4 SCOUT's NETWORK AND INFORMATION SECURITY PROGRAM 9
4.1 Organizational Location and Reporting Chain 9
4.2 Network and Information Security Staff 10
4.3 Organizational Interfaces 10
4.3.1 Internal Interfaces 10
4.3.2 External Interfaces 12
4.4 Corporate Information Security Policies and Procedures 12
4.4.1 Fundamental Corporate Proprietary Information Security Policy 13
4.4.2 Information Classification 13
4.4.3 Computer Systems Security 14
4.4.4 Network Security and Acceptable Use 14
4.4.5 Computer User IDs and Passwords 14
4.4.6 E-mail Policy 14
4.4.7 Internet Services 14
4.4.8 Social Engineering 15
4.5 Information Security Program Costs 15
4.5.1 Costs Associated with Incidents 15
4.5.2 Cost for Sustaining the Environmental Safety and Security Program 15

5 SCOUT BUSINESS CASE PROCEDURES 17

6 SCOUT MANAGEMENT VIEW OF SECURITY 20

LIST OF TABLES

Table **Page**

1 Business Units 4
2 Information Classification 14

DCA100-95-D-0104
Delivery Order No. 10
Information Security Business Case
Case Study #3-SCOUT

1. INTRODUCTION

In recent years, information and telecommunications technology and services have expanded at an astonishing rate, in terms of the technology and implementation. The public and private sectors increasingly depend on information and telecommunications systems capabilities and services. In the face of rapid technological change, public and private organizations are also undergoing significant changes in the way they conduct their business activities, including the use of wide area networking via public networks. These changes include mandates to reduce expenses, increase revenue, and at the same time compete in a global marketplace. Even under prosperous economic times, security has not been easy to sell to upper management unless the organization has been the victim of a major security incident. In today's business environment it is even more difficult to obtain senior management approval to justify the expenditure of valuable resources -- yet, this expenditure is necessary to "guarantee" that a potentially disastrous event will not occur and affect the ultimate survivability of an organization.

SAIC has been tasked by the Office of the Manager, National Communications System (OMNCS), Customer Service and Information Assurance Division, Information Assurance Branch (N53) under the Defense Information Systems Agency (DISA) contract DCA100-95-D-0104, Delivery Order 10, to provide the Government with a report and briefing supporting the justification of funding network security related programs. The purpose of Task 2 of this delivery order is to research, develop, produce, write, and publish three individual case studies of organizations which have been the victims of significant intrusions and have initiated significant programs afterward to improve security within their networks. This report represents the third of the three case studies.

To protect the anonymity of the organizations in the case studies, a code name has been assigned to each organization. The code name of the third case study organization is SCOUT.

1.1 Purpose of the Project

The overall purpose of the Information Security Business Case project is to research, develop, produce, write, and publish a Business Case for Security. The project consists of performing research on three organizations that have been the victims of significant network intrusions or have initiated significant programs to improve security within their networks for other reasons such as deregulation of an industry sector or direction of a corporate board of directors. The final product will be a "generic" approach/methodology for justifying network and information systems security expenditures.

1.2 Approach for SCOUT Case Study

The first step in performing the SCOUT case study was obtaining the consent of the organization's senior management to be a participant. The case study point of contact was the Director of Network and Information Security. Once an oral agreement was obtained, SAIC and the participant executed a non-disclosure agreement to ensure the organization's anonymity. SAIC developed a questionnaire guide to be used during the initial data collection effort. A team of three SAIC personnel conducted a 1 day on-site visit to the participant organization and interviewed the point of contact using the questionnaire guide. During the interview, the SAIC team identified several documents and requested copies. Documents collected during the interview included policies, procedures, code of conduct statements, and business case procedures. Several follow-up telephone conversations were held between the SCOUT point of contact and the SAIC principal investigator to answer questions and to obtain additional data relevant to the case study. Background material concerning the participant organization was obtained both from the participant and from open sources.

1.3 Overview of the Report

Section 2 describes the business services and the technical and operational environments of SCOUT. Section 3 depicts the activities that motivated SCOUT to develop a network and information security program. Section 4 provides a description of the evolving network and information security program, including the security organization and the security policies. Section 5 describes the current business case analysis process used by SCOUT. Section 6 provides the lessons learned by SCOUT management as a result of the network intrusion.

2. OVERVIEW OF THE SCOUT ORGANIZATION

2.1 Description of the Business

SCOUT is a U.S.-based international company with a diverse range of information processing systems. SCOUT's long-distance, local telephone, Internet service, and wireless subsidiaries provide integrated communications services to several million businesses and residential customers nationwide. The company's combined wireless, wireline local, and long-distance revenues rank it amongst the top 10 telecommunication companies in the United States today. The company provides local and global calling services, wireless communications, network and information management services, and Internet Services and teleconferencing. It offers the critical trio of telecommunications services: long distance, local, and wireless. With the integration of SCOUT's newest companies, it is launching a nationwide effort to extend this full range of services to all of its customers, while:

- Enhancing a self-healing fiber-optic nationwide network
- Expanding its enhanced telecommunications services platform by adding new network control processors and various gateway, billing and interface servers (the platform consists of Signaling System 7 (SS7) links connecting SCOUT's UNIX®-based client server computers and extremely reliable, high-capacity long distance switches)
- Installing a client-server based billing and collection system with integrated customer care interfaces.

SCOUT is organized into eight business units. Table 1 provides the units and their primary services.

Table 1. Business Units

BUSINESS UNIT	SERVICES
Wireless Unit	Provides wireless services such as cellular phone and paging.
Internet Services	Provides a full range of information, communications and publishing services.
Long-Distance Services	Local, competitive local, interstate and international calling services.
Network Services	Builds, installs, repairs, and manages telecommunications network; wholesales network/database/billing services for SCOUT and SCOUT business customers.
Calling Card Services	Provides pre-paid and post-paid calling card service to consumers.
Local Exchange and Alternate Exchange Carrier Services Group	Serves residential and business customers inside and outside of its operating territories.
Teleconferencing Services Group	Packages advanced voice, data, and video teleconference services for business.
Operator Services	Provides retail operator services for SCOUT customers and wholesale operator services for major exchange carriers across the United States.

2.2 Description of Network and Information Systems Environment

The information and network technology used to support SCOUT's corporate backbone network environment and all of the core business units is a widely distributed, heterogeneous environment. It includes a plethora of legacy platforms and systems from the many acquisitions and mergers initiated by SCOUT over the last few years. The environment consists of, but is not limited to, the following technology:

- Intel-based Personal Computers running DOS and Windows
- LOTUSNotes Server
- Welfleet 7.X Routers
- Cisco Routers
- AS-400 Servers
- Sun Solaris 2.5 Workstations
- IBM AIX® 4.1.4
- Firewalls

- Analog modems, cellular packet data modems, and modem pools tied to SCOUT's Local Area Networks (LANs) and networked subsidiary environments
- Nortel DMS-250 Supernode™
- IBM MVS.

The SCOUT corporate distributed backbone network supports various applications and enterprises, including the business units identified in Table 1. The backbone Wide Area Network (WAN) consists of the many sub-networks of the SCOUT subsidiaries tied together by LANs and WANs. This provides connectivity to mainframe legacy operations support systems, network elements, data communications networks, and commercial information and services network provider platforms. The information technology applications include a number of telephony business critical functions, such as a new client-server billing system. The new billing system operates on IBM's AS-400 servers running AIX, and Windows NT supporting Relational Database Management (RDBMS) technology supporting Microsoft SQL Server, Oracle®, and Informix.

3. MOTIVATION(S) FOR ESTABLISHING SECURITY PROGRAM

The security program within SCOUT developed primarily as a byproduct of SCOUT's unprecedented growth and integration of companies, systems, and centers. Other motivations were increased competition, risks, and threats in the globally connected world of cyberspace where connectivity to one network implies connectivity and trust relationships to many. In developing the organization, SCOUT senior management tasked its new security director to develop a visionary, cost-efficient, multi-discipline, integrated (horizontal and vertical) model approach to their corporate *security, safety, and soundness* including information protection and business operations assurance. That approach evolved into the SCOUT Infrastructure and Facilities Safety and Security mission; the establishment of an information and network security sub-mission; and the organizational development of an inter-organizational and interdepartmental information security structure, known within SCOUT as the Pro-active Security Program (PSP). The primary function of PSP is to leverage security into the planning and operations phase of each information technology (IT) project throughout SCOUT. PSP is interdepartmental, with core team members consisting of the following SCOUT entities:

- IFSS personnel responsible for policies and investigations
- SCOUT IT personnel throughout the operating units responsible for incident response and reporting
- SCOUT network systems personnel throughout the operating units responsible for information security.

A secondary motivation for the establishment and expansion of SCOUT's PSP network and information security program was to allow SCOUT operations the ability to prevent, detect, contain, and deter incidents or intrusions into the internal business platforms and customer service IT environments. In the last year, several significant incidents were recognized and satisfactorily contained through formal and informal PSP actions and initiatives.

A denial of service attack against its Internet Service Provider (ISP) entity, SCOUT.net, caused the loss of an Internet service component to the public. The incident involved an attack technique known as a TCP SYN attack, in which a perpetrator's host transmits a large volume of connection requests that cannot be completed because the intended addresses for the connections are bogus. This caused the connection queues of the ISP server (in this case the targeted component server) to quickly overflow, denying service to legitimate customers for more than 3 days. The attack was immediately detected when the loss of service occurred. The PSP team contained the incident; the suspected perpetrator was identified; and his access privileges were suspended. The case has been referred to the National Computer Crime Squad of the Federal Bureau of Investigation (FBI) for criminal prosecution. The economic losses resulting from the incident exceed twenty thousand dollars in lost services and additional labor costs to detect, isolate, investigate and mitigate the intrusion. Had the interdepartmental PSP 24-hours-per-day, 7-days-per-week reporting, incident response, and investigation capability not been in place, the impact could have quickly spread to other SCOUT ISP services and servers in a fashion similar to the denial of service losses experienced by other ISPs[1] and websites.

A second incident mitigated by the PSP team involved insiders who, in anticipation of a work stoppage, changed the boot-up (BIOS) passwords on several critical business servers. The PSP team, working around the clock, quickly determined the nature of the rogue password changes, identified the suspected perpetrators, and reset the systems back into normal operation. The case resulted in disciplinary actions, including dismissal of many individuals involved for violations of SCOUT's *Code of Ethics and Business Conduct*. Although there were labor costs associated with mitigating this incident, the costs were not documented because the case was never brought to prosecution.

A third incident involved a recently separated SCOUT ISP employee, who had been dismissed for *Code of Ethics and Business Conduct* violations involving the downloading of obscene contraband images from the Internet onto his workstation at work in the SCOUT ISP offices. Although the employee's ISP account and access rights were terminated, they were inadvertently re-established when the ex-employee reactivated the ISP account as a personal account. Because an error identified the personal account as a company account, the employee's privileges were incorrectly restored along with the ISP account. The employee, realizing the situation, accessed SCOUT internal systems, changed users' Distributed Computing Environment (DCE) passwords

[1] In early September 1996, an unknown criminal hacker attacked the PANIX ISP in New York City. The intruder used a similar TCP/SYN-flooding attack, denying service to legitimate users and forcing the ISP to take its servers out of service for an extended period until software patches to alleviate the attack had been installed. Identical attacks have incapacitated several other service providers in the past few months.

and eavesdropped on electronic communications within the IT distributed networking environment. These activities were discovered when several customers phoned the help desk, indicating that they were unable to access their ISP accounts. Although the PSP team acted swiftly to mitigate the problem, the weakness in systems controls involving exiting employees was apparent. The two incidents, before and after the employee was terminated, supported the need for more specific policy and procedure regarding SCOUT *Computer and Network Acceptable Use and Exiting Employee Separations* processes. Costs associated with this incident include labor to mitigate the incident, minimal loss of service, and labor to develop new Exiting Employee Separations processes. Because this incident was never brought to prosecution, the specific cost details were not documented by the SCOUT organization.

In all, SCOUT's PSP team investigates and resolves 200 to 300 incidents per year. Costs for specific incidents are not documented unless prosecution is pursued.

4. SCOUT’s NETWORK AND INFORMATION SECURITY PROGRAM

The SCOUT Infrastructure and Facilities Safety and Security mission and the information and network security sub-mission, known within SCOUT as the PSP, was established to leverage security into the planning and operations phase of each IT project across SCOUT. PSP provides a policy, guideline, awareness, implementation, and compliance and reporting vehicle to SCOUT and its subsidiaries and project managers nationwide. Because of IFSS-led PSP initiatives on access control to key facilities, including central offices, access control security costs related to these operations have been reduced by 58 percent while effectiveness over key control based systems and guards has been increased by nearly 100 percent. Given the diverse nature of the IT operations, significant capital expansion programs, and related audit findings, SCOUT intends to undertake the following critical steps:

- Identify and document points of access to SCOUT’s networks
- Conduct a risk assessment of the SCOUT IT network architecture and applications
- Perform a vulnerability accessibility test of the identified access points and applications
- Assess impact of inappropriate access to those points
- Provide a confidence level that all access points were identified
- Provide tools to identify and document changes in access points
- Provide possible solutions to reduce vulnerabilities
- Provide input to future SCOUT network architectures to address security.

Other critical steps are also under consideration. The objective of SCOUT’s PSP information security strategy is to ensure that security has been considered adequately from the start within the competitive business environments of SCOUT’s strategic markets. The goal is to implement security solutions in an efficient, automated, customer-friendly approach that is available anywhere at any time.

4.1 Organizational Location and Reporting Chain

The Assistant Vice President (AVP) of SCOUT IFSS reports directly to SCOUT’s Chief Financial Officer (CFO)/Chief Operations Officer (COO). The office of the CFO/COO reports directly to the SCOUT Chief Executive Officer (CEO) and to the Board of Directors. The

CFO/COO is charged with providing updates on security to the Audit Committee of the Board of Directors.

In addition to network and information security responsibilities, the AVP of SCOUT IFSS coordinates policy and procedures for information classification and for protection and risk management of proprietary information . The risk management organization focuses on business continuity and insurance relative to information technology, and reports to the AVP of SCOUT IFSS. Also reporting to the AVP-IFSS is the Manager, Systems Security and Technology, who serves as the IFSS core team PSP member.

4.2 Network and Information Security Staff

Three of the thirteen SCOUTS IFSS staff members are on the network and information security PSP staff within SCOUT IFSS. The new SCOUT IFSS Information Security *Computer and Network Acceptable Use* booklet, which develops the inventory of employee access privileges, and the *Exiting Employee* Checklists are but a few of the initiatives and responsibilities of this central staff. Examination of these draft documents and concepts revealed *state of the practice* insights to help minimize and manage risk. PSP's main role is as an interdepartmental collaborator. Most of the PSP team resides within the SCOUT Information Technology organization. The SCOUT IT PSP core member resides in the Information Technology Security & Control Organization, reporting to the head of the SCOUT IT organizational entity. The Information Technology Security & Control Organization is responsible for day-to-day information security practice and procedures, including incident response.

4.3 Organizational Interfaces

4.3.1 Internal Interfaces. Internally, the AVP-IFSS has a very good liaison, and usually weekly contact (if not daily), with senior management and Internal Audit. The Manager, Systems Security and Technology interacts with the various PSP team members in the SCOUT subsidiaries and departments. The AVP-IFSS frequently maintains additional informal liaison with the business operating units. The AVP assists operating units in discussing environmental, safety, or security issues pertinent to their business activities and those of their employees. The AVP also maintains close contact with the internal Audit Committee of the Board of Directors.

The PSP program is a well-developed organizational interface created to ensure that security concerns are integrated into all aspects of SCOUT's business. The PSP mission is to "Ensure that SCOUT's Information Systems and Communications Networks are properly controlled, safeguarded, and monitored to provide the necessary levels of integrity, confidentiality, and availability." To meet this mission, the PSP program has established a set of goals:

- Anticipate risks to all electronic systems and mitigate those risks to acceptable levels through the cost-effective use of technology and administrative controls
- Protect assets adequately from unauthorized use or disclosure
- Ensure that authorized, aware users have access to electronic resources and understand their responsibility to protect them
- Detect unauthorized access as soon as possible to minimize potential loss.

PSP operates with greater influence and responsibilities than do other internal security organizational interfaces. The following are identified as specific PSP responsibilities:

- Establish and maintain protection, countermeasure, and management control policies.
- Identify and assess risks to Information Systems and Communication Networks. Identify anomalies and weaknesses in systems, and determine actions necessary to upgrade substandard system and network controls.
- Develop programs to increase user awareness of the need to protect information systems and communication networks and how to use the systems effectively.
- Provide standards by which systems can be designed with the necessary security controls available.
- Evaluate information systems and communications networks for policy compliance and security effectiveness.

PSP has established a network of members that spans the SCOUT organization. These members work in the following functional areas, as well as others:

- LAN Operating Systems
- Corporate Security
- Database Administration
- UNIX Systems Administration
- Business Recovery Management
- Network Connectivity
- Information Security
- Cellular Fraud and Roaming
- Attorney/Legal
- Network Security
- Customer Support
- Toll Fraud Systems Management
- Internet Management
- Cellular MIS Management
- Network Engineering
- VAX Operating Systems
- AS-400 Network Security
- Enterprise Network Management
- Network Services
- MIS Management
- Telephone Network Engineering
- Proprietary Information Coordinator
- Inter-platform Security Administration
- Mainframe Security Administration
- Application Architecture Management
- Human Resources.

4.3.2 External Interfaces. SCOUT belongs to a variety of external information security groups. The primary ones are the American Society of Industrial Security (ASIS) and an ad hoc risk management group sponsored by SCOUT's primary insurance carrier. The AVPIFSS receives and responds to numerous inquiries from the telecommunications industry and the insurance industry, as a result of the unique nature of SCOUT's multidiscipline business-centric approach to Environmental, Safety, and Security.

4.4 Corporate Information Security Policies and Procedures

SCOUT has a new set of Corporate Information Security policies and guidelines. The recently issued policies and guidelines now fully address the changing risk management environment and concerns recognized during the PSP responses to the security incidents highlighted earlier in this case study. The policies govern the acceptable use of and protection of all SCOUT information and all computing and networking resources. The guidelines are based upon an expansion of both the SCOUT Vision Statement and the policies contained within the SCOUT Code of Ethics and Business Conduct. The set of guidelines and policies state the fundamental information security rules, expectations, rewards, and penalties for non-compliance and responsibility to acknowledge and comply with the stated principles and policies. The SCOUT IFSS Information Security *Computer and Network Acceptable Use* booklet, which addresses eight specific areas, outlines:

- The need for security policies and guidelines and employee obligations and contributions
- Acceptable use of information, computer and network resources
- Use of and guidelines for userids and passwords for access to systems
- DOs and DON'Ts to remember
- E-mail Policy, privacy expectations, cautions and proper use
- Software use and copyright protection
- Internet Services, conventions, expectations, and acceptable use
- Guarding against social engineering and other interpersonal hacking incidents
- PSP team support and points of contact
- Network acceptable use policy examples
- Enforcement and violation reporting.

4.4.1 Fundamental Corporate Proprietary Information Security Policy. The fundamental policy states that, as part of achieving the SCOUT Vision in a competitive marketplace, proprietary information is a corporate asset, which must be managed properly. The policy states that all employees protect the integrity of SCOUT's business and customer information at all times during and after their employment with SCOUT.

4.4.2 Information Classification. This policy identifies and defines two data classifications that categorize all proprietary data. The categories are: **Proprietary** and **Private** Restricted Distribution, Use and Availability (see Table 2). Information classifications are described in a *Proprietary Information Handbook* that outlines how SCOUT defines proprietary information, how to identify it, mark it, store it, and destroy it.

Table 2. Information Classification

CLASSIFICATION	DEFINITION
Proprietary	Not for use or disclosure outside SCOUT operating companies except under written agreement.
Private	Information intended solely for use by those authorized employees of SCOUT operating companies who have a need to know the subject matter. Disclosure to others is strictly prohibited.

4.4.3 Computer Systems Security. This policy outlines acceptable use policies for computer systems, employee responsibilities for safeguarding computing resources, and consent to monitoring for performance, integrity, and policy compliance. It also forbids the installation of software on SCOUT computers without prior authorization.

4.4.4 Network Security and Acceptable Use. This policy states acceptable use policies for SCOUT network resources and sets security requirements for network use such as proper use of system IDs, publication (i.e., Intranet) restrictions, and examples of illegal activities.

4.4.5 Computer User IDs and Passwords. These policy outlines user responsibilities for IDs assigned to employees to include safeguarding of the ID, compliance with password changing requirements, password configuration requirements, and a series of DOs and DON'Ts.

4.4.6 E-mail Policy. SCOUT corporate e-mail policy states that e-mail is for business use only and all e-mail is the property of the corporation. Personal privacy is not intended or implied with e-mail use and if a subject or tone is not appropriate for a memo, it is not appropriate for e-mail messages. It also notifies employees of e-mail password purposes (for authentication only) and outlines common
e-mail mistakes.

4.4.7 Internet Services. The policy states that any access to Internet resources provided by SCOUT to its employees fall under acceptable use policies. Access to the Internet is provided for business use only.

4.4.8 Social Engineering. Realizing the threat of social engineering with the telecommunications industry, this section outlines potential social engineering techniques and advises employees to verify the identity of all callers requesting assistance or information. It also sets forth a reporting requirement for any social engineering attempts or suspicious phone calls fielded by an employee.

4.5 Information Security Program Costs

4.5.1 Costs Associated with Incidents. The costs associated with the primary incident researched (SYN attack) for labor and lost services were between $20,000 and $25,000. SCOUT calculated the cost of lost service at approximately $13,000; this estimate is based on the average number of users applied over the outage period. Labor costs were calculated at approximately $9,000 from the time of detection of the incident to restoration of service; this calculation includes investigative labor costs. In this case, the loss consisted of both lost revenues and the investigation and recovery costs. Owing to the IFSS rapid **detect, react, contain** mechanisms, the service loss was less than the investigation and recovery cost. SCOUT IFSS believes that had the incident continued longer than 1.5 days, the investigation costs would have continued to escalate but at a lesser rate than the service loss costs. SCOUT, like its peers in the industry, suffers from several incidents; however, the cost impact is reduced significantly by their capability to contain and mitigate each unique incident that arises. This capability is a direct result of SCOUT's investment in the security program and established organizational interfaces with established roles, responsibilities, and accountabilities.

To put the example in perspective, a similar SYN attack was waged against Web Communications, Inc. (Webcom) in December 1996. One customer of Webcom alone (out of 3000 total) indicated that the denial of service SYN attack against Webcom cost his business $20,000.[2]

4.5.2 Cost for Sustaining the Environmental Safety and Security Program. The cost of the SCOUT security department is distributed and segmented based upon functional are; therefore, it is difficult to track precise cost data related to information security and protection.

[2] "FBI probes charges of sabotage at Calif. Web server," Reuters, December 20, 1996.

The AVP Infrastructure and Facilities Safety and Security indicated the annual cost of the IFSS functionality to be approximately $1.8 million. Given the number of incidents with which the SCOUT organization is faced (and which SCOUT mitigates effectively at minimal cost) and given the annual savings brought about by programs such as the new access control and identification card system, it is apparent that the program, in effect, pays for itself. Plans to initiate an internal 20 percent overhead charge for IFSS continued services will allowed the program to create revenue that, when coupled with savings and threat mitigation, should exceed the cost of sustaining the program.

In addition to the self-funding mechanisms described above, IFSS has an extensive cost-containment program in place, which has resulted in significant six-figure results to date.

5. SCOUT BUSINESS CASE PROCEDURES

SCOUT is a rapidly growing commercial enterprise competing in a rapidly changing marketplace that is largely driven by rapid changes in communications technology, regulations, and coupled with cost reductions (and implicitly increased productivity) to satisfy the equity of its shareholders and Wall Street). Both market competitiveness as well as scrutiny from state and federal regulatory agencies drive pricing of integrated communications services. While largely based on rates established by the public utility commissions among more than 30 states and more than 12 foreign countries, SCOUT's integrated communications services, pricing and profitability growth is also significantly influenced by deregulation. SCOUT's policies and procedures for capital expenditures are largely evolving with its rapid growth and customer demand.

SCOUT's investment decision processes consist of three distinct types of activities that are identifiable with three basic hierarchical organization levels (coupled with available budgets):

- CEO and Board of Directors for very large capital investments, where CEO/COO/CFO approve investments that exceed a $1 million threshold
- Capital Investment Council, responsible for review and approval of capital investment decisions that exceed $500 thousand but are less than $1 million
- Corporate directors and certain operating units who have signature authority for investments greater than $100 thousand but less than $500 thousand.

Although the policies and procedures establish clear thresholds, the context of decision support documentation appears less formal and structured, and may involve selected individuals from lower organizational levels. Context and structure appear to be dictated by the general purpose, the levels of the decision making, and the schedule of authority within the organization hierarchy.

The CEO, COO, CFO, and Board of Directors, while focusing on capital investments exceeding $1 million, also address the equally important functions of securing and enhancing their competitive advantage. One aspect has been the acquisition of profitable businesses in communications service markets, principally in new markets and secondarily in the expansion of existing markets to ensure critical mass. A less formal process exists for keeping this level of participants informed of lower-level decisions in the aggregate, and of potential liabilities that may affect the balance sheet.

The next two levels seem to focus on communications equipment, related software, and service investments. At these levels, the emphasis is on those investments that maintain and preserve the systems, i.e., those items that are "critical to the continuity of the business." Increased productivity (i.e., efficiency) is a significant decision criterion.

The fundamental horizon in the capital budget, which is essentially a 1-year document but identifies potential commitments that may extend another 1 to 2 years. Long-range planning is a 3-year horizon. This is short by most standards; 5 or more years is generally the norm. This shorter long-range horizon may be consistent with rapid changes in technology, for example, processors, a significant portion of their equipment suites — both primary (e.g., ISP business unit) and secondary (i.e., office applications). The recent addition of a formal strategic planning function at the corporate level may change this perspective somewhat.

Further, SCOUT's ESS actual budget is relatively small; therefore, they leverage investment in security from budgets of the operating departments and subsidiaries. To quote, the effect of this investment strategy is "to buy the pie one slice at a time." Through this process they have also begun to consolidate investments in a common set of "standard" equipment and software that remains interoperable with the diverse "legacy" suites. The operating subsidiary/unit is their target of opportunity for risk management efficiencies and compliance. They are consolidating and standardizing facility systems by effectively showing the operating unit that it is cost effective and that most investments will pay for themselves in 1 to 2 years.

While there are no apparent investment hurdles, a payback of 2 years or less seems to be the decision criteria. In several examples, it was less than a year. As this organization matures at the corporate level, the Strategic Planning group and finance/budget group is likely to implement other criteria such as Net Percent Value.

Though there is no apparent standardized format for business case analysis within SCOUT, the formal investment documentation inspected required the following:

- Title
- Objective and Description
- Alternatives
- Analysis, Conclusion, and Recommendations
- Implementation Scheduling
- Interfaces, Policies, Procedures, Signoff, Concurrence
- Attachments.

Further insights regarding business case models for investment will probably be obtained during the interview with SCOUT senior management.

6. SCOUT MANAGEMENT VIEW OF SECURITY

Two senior officers of SCOUT were interviewed concerning security issues. The interview addressed the following questions:

- What are senior management perceptions of the security risks?
- How much of a “wake-up call” was the intrusion incident?
- What security concerns were raised as a result of the intrusion?
- What are the security concerns regarding Open Networks and the Telecom Act of 1996?
- What is the approach for sustaining network and information security over time?
- How will the expense of maintaining the program be justified?
- What is the organization comfort level with what you have done and your plans for the future?
- What is the business model for addressing security risks?
- What are the lessons learned from the incident?

SCOUT’s senior management is cognizant of the risks its telecom operations, customers, and partners face. They view the effective mitigation of those risks through the IFSS PSP program as part of doing business in today’s competitive open market environment; they expressed some reservation as to whether the effort was similar to legal and regulatory compliance programs. While they understood the need and the value of the security program, its voluntary nature made it distinct and more discriminatory than compliance programs linked to federal and state laws. They also expressed some concern as to its benchmarking and balance with the developing risk. They felt that the mandates of unbundling, interconnection, and co-location associated with the Telecom Act of 1996 and the Open Market competitive environment the company is supporting will bring additional risks to Local Exchange operations, customers, and reliability. From a financial standpoint SCOUT does not want to spend more on security than its competitors do, but they are willing to take the initiative to provide adequate resources and support to prevent damaging incidents or exposures. They did not view computer security compliance on the same level as financial reporting, anti-trust, environmental, safety, sexual harassment and other offenses governed under the U.S. Federal Sentencing Guidelines. They would, however, support such compliance program expansion to include computer security, as it relates to fiduciary positions of trust, if it were mandated or otherwise proscribed by federal or state law.

SCOUT senior officers also stressed the importance of giving the security program direct access to senior management to ensure that an open dialogue regarding security issues is maintained. Security issues are discussed and debated between the senior management and the Director of IFSS, so that decisions can be based on informed discussion. Senior management maintains that they are concerned, but not paranoid, about security; this perspective gives the security program flexibility to make wise investments.